



Facultad
Militar
Conjunta

OBSERVATORIO ARGENTINO DEL CIBERESPACIO

Director del Proyecto: BM (R) Alejandro Moresi
Codirector: TC (R) Ing Carlos Amaya
Edición: Bib Alejandra Castillo



ISSN: 2718-6245

<https://undef.edu.ar/fmc/ciberespacio/boletines.php>



AÑO 9 N°61
Mayo-Junio 2026

OAC Boletín NÚMERO 61, mayo-junio 2026

“la transparencia es insuficiente para anular por completo la influencia de los videos deepfake”

<https://www.nature.com/articles/s44271-025-00381-9>

Tabla de Contenidos

ESTRATEGIA.....	3
IA, Drones robots, IA no todo es tecnología en la guerra futura	
Los chips estarían redefiniendo el poder global	
CIBERGUERRA.....	4
Estrategia de preparación ante la IA general para reducir el riesgo estratégico y promover la estabilidad en la transición a la inteligencia artificial general.	
CIBERSEGURIDAD	4
Ciberataques a través de la cadena de suministros	
CIBERDEFENSA.....	4
Inteligencia artificial aplicada a la defensa más allá de los titulares	
La capacidad de gestión de la IA en cuestiones de seguridad y militares	
CIBERCONFIANZA	6
Los videos IA y deepfake	
TECNOLOGÍA	6
Mapa de la industria militar de IA	
CIBERFORENSIA	7
Informes de Vulnerabilidades	



EVENTO 55 Jornadas Argentinas de Informática (JAIIO)	7
Lecturas, Videos y Podcats.....	7
1. Podcast Guerra Cognitiva: https://global-strategy.org/guerra-cognitiva-i/	
2. Operaciones en el Ambiente de la Información Libro en formato digital disponible en: https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/CEFADIG_b2ce737fe7427cb279d7cb6ef4bd53c8	
3. La ciberseguridad es ahora una prioridad en las salas de juntas: https://www.youtube.com/watch?v=Jgu4VY7zyAg La empresa agente: cómo los agentes de IA están transformando los negocios con Adam Evans de Sale.. https://www.youtube.com/watch?v=bsxrTa9YL3Y	
CYBER AR -Tercera circular.....	8

El Observatorio Argentino del Ciberespacio (OAC), es un micro-sitio de la
Facultad Militar Conjunta de las Fuerzas Armadas,
editado y publicado por el Instituto de Ciberdefensa de las Fuerzas Armadas
URL: <https://undef.edu.ar/fmc/ciberespacio/boletines.php>

Esta publicación mensual se encuentra inserta en el
Nodo Territorial de Defensa y Seguridad de la Red Nacional de
Nodos Territoriales (NT) de Vigilancia Tecnológica e Inteligencia Estratégica (VTeIE) del
Ministerio de Ciencia, Tecnología e Innovación de la Nación y es
administrado por el Centro de Estudios de Prospectiva Tecnológica Militar
“Grl Mosconi” de la Facultad de Ingeniería del Ejército Argentino.
Nuestro objetivo se reafirma en la intención de llevar a la comunidad ciberespacial
distintas perspectivas de este nuevo ambiente operacional,
aportando novedades, reportes e informes que permitan a la comunidad educativa
y a la sociedad en general conocer más acerca del mismo.



ESTRATEGIA

IA, Drones robots, IA no todo es tecnología en la guerra futura

La transformación de la guerra moderna no es meramente táctica, sino fundamental, y exige una revisión de la doctrina militar, el derecho internacional y la propia naturaleza del poder estatal en el siglo XXI. A medida que la tecnología de precisión se vuelve más accesible y los sistemas autónomos más capaces, el desafío consistirá en mantener el control humano sobre la conducción de la guerra, preservando al mismo tiempo los principios humanitarios que han guiado las relaciones internacionales durante más de un siglo.

La historia militar ha demostrado a menudo que los conflictos están menos determinados por una innovación aislada que por la combinación de factores estructurales. La logística, la capacidad industrial, la cohesión social, la organización de las fuerzas armadas y la resiliencia económica suelen desempeñar un papel decisivo, a veces variables menos visibles pueden resultar decisivas, como la moral de las tropas, la cohesión social, la cultura organizativa de las fuerzas armadas, la capacidad de adaptación doctrinal y la relación entre las autoridades militares y políticas.

El caso de Ucrania parece ser un excelente ejemplo: cohesión nacional, mando descentralizado, capacidad de innovación táctica y la rápida integración de tecnologías civiles (drones comerciales, plataformas de comunicación como Telegram y Starlink). Esta “adaptabilidad distribuida” permitió a Ucrania compensar las importantes asimetrías iniciales en potencia de fuego y recursos.

<https://theconversation.com/drones-robots-ia-la-technologie-suffit-elle-a-preparer-la-guerre-du-futur-278805>

<https://blogs.icrc.org/law-and-policy/2025/05/22/the-shifting-battlefield-technology-tactics-and-the-risk-of-blurring-lines-of-warfare/>

<https://www.csis.org/analysis/chapter-9-technological-evolution-battlefield>

Los chips estarían redefiniendo el poder global

Durante décadas, la cadena de suministro de semiconductores pareció ser uno de los mayores triunfos de la globalización. Era un sistema transcontinental complejo y tan eficiente que sus vulnerabilidades pasaban prácticamente desapercibidas. Esa certeza se ha desvanecido. Una serie de crisis, desde la escasez provocada por la pandemia hasta la escalada de tensiones entre Estados Unidos y China, ha revelado que la tecnología más esencial del mundo depende de una cadena de suministro que se encuentra en una situación de gran inestabilidad geopolítica. Durante décadas, los semiconductores habían permanecido fuera del radar público. Invisibles dentro de teléfonos móviles, servidores o electrodomésticos, parecían pertenecer a un mundo técnico reservado a ingenieros y especialistas, sin embargo hoy son el eje de una economía global hiperconectada.

<https://theconversation.com/los-chips-estan-redefiniendo-el-poder-global-279486>

<https://www.microwavejournal.com/articles/45564-chips-power-and-geopolitics-the-race-to-control-the-future>

<https://www.vanderbilt.edu/national-security/2025/05/09/the-next-great-power-struggle-control-over-chips-and-computing/>



CIBERGUERRA

Estrategia de preparación ante la IA general para reducir el riesgo estratégico y promover la estabilidad en la transición a la inteligencia artificial general.

En un escenario global marcado por la carrera hacia la Inteligencia Artificial General, este análisis propone un giro estratégico clave: en lugar de competir por llegar primero, plantea cómo evitar un desastre. Inspirado en la lógica de estabilidad de la Guerra Fría, el concepto de “Resistencia a la IAG” abre un debate urgente sobre disuasión, resiliencia tecnológica y control de riesgos en un futuro dominado por la IA. Una lectura esencial para comprender los desafíos estratégicos emergentes y las decisiones que podrían definir el equilibrio de poder del siglo XXI.

<https://www.rand.org/pubs/perspectives/PEA4347-1.html>

CIBERSEGURIDAD

Ciberataques a través de la cadena de suministros

Los ciberdelincuentes están accediendo cada vez más a las organizaciones no a través de sus sistemas principales, sino mediante sus proveedores más vulnerables, y muchos de estos incidentes no se reportan públicamente. Así lo afirma Unit 42, el equipo de inteligencia de amenazas y respuesta a incidentes de Palo Alto Networks, que destaca que más de uno de cada cuatro ciberataques (28%) investigados en Europa durante el último año tuvo su origen en brechas de terceros. Esta cifra podría ser incluso mayor, ya que muchos ataques que comienzan en terceros no se identifican ni se reportan como incidentes de la cadena de suministro, lo que oculta la magnitud real del problema.

<https://revistabyte.es/actualidad-it/ciberataques-en-cadena-de-suministro/>

CIBERDEFENSA

Inteligencia artificial aplicada a la defensa más allá de los titulares

La integración masiva de inteligencia artificial está transformando la ciberdefensa y las operaciones militares a una velocidad sin precedentes. Mientras sistemas avanzados automatizan la detección de vulnerabilidades y el gasto en tecnologías autónomas alcanza cifras récord, surgen interrogantes críticos: ¿estamos sacrificando la deliberación humana por la rapidez operativa? Desde la dependencia estratégica de firmas tecnológicas externas hasta los riesgos éticos de la selección automatizada de blancos, analizamos el complejo equilibrio entre innovación y control.

Exploremos cómo esta carrera por la supremacía tecnológica redefine la seguridad nacional y la necesidad urgente de transparencia para proteger tanto la eficacia operativa como los derechos fundamentales.

<https://www.rusi.org/explore-our-research/publications/commentary/defence-ai-beyond-headlines>

<https://www.brennancenter.org/our-work/research-reports/militarys-use-ai-explained>

<https://www.brennancenter.org/our-work/research-reports/business-military-ai>



<https://www.rusi.org/explore-our-research/publications/commentary/ai-enabled-vulnerability-discovery-reshaping-national-cyber-defence>

La capacidad de gestión de la IA en cuestiones de seguridad y militares

Basándose en los avances recientes, la inteligencia artificial (IA) con agentes es un paradigma tecnológico emergente y la próxima ola en el desarrollo de la IA que permite a los agentes perseguir de forma autónoma objetivos complejos e interactuar entre sí con una supervisión humana mínima mediante la integración de amplias capacidades de modelos de lenguaje. A través de agentes cada vez más autónomos, la IA con agentes está transformando el panorama de la IA, pasando de ser una herramienta pasiva de apoyo a un ejecutor activo que puede definir y tomar decisiones en nombre del usuario. Si se implementa con éxito, la IA con agentes amplía el alcance, la escala y la complejidad de los posibles casos de uso de la IA, incluso en ámbitos donde la automatización tradicionalmente ha resultado difícil, al tiempo que transforma la colaboración y la delegación entre humanos y máquinas. Sin embargo, aunque el rendimiento de los agentes de IA parece estar aumentando rápidamente, muchas aplicaciones reales de IA con agentes aún se encuentran en fase experimental, y su eficacia ha resultado bastante limitada. Por lo tanto, es importante ir más allá de la euforia que la rodea y evaluar críticamente su estado actual y sus capacidades previstas. El análisis que se presenta en este documento de Ginebra tiene como objetivo proporcionar una mejor comprensión de estas cuestiones, trazando un mapa del panorama en rápida evolución de la IA con agentes, desde sus fundamentos técnicos hasta sus posibles implicaciones estratégicas.

La IA con agentes posee un potencial inherente de doble uso que transformará tanto las aplicaciones comerciales como las militares. Sin embargo, persisten las incertidumbres sobre sus capacidades futuras y el ritmo de su desarrollo, así como las limitaciones técnicas existentes y otras barreras que podrían ralentizar el despliegue de agentes y dificultar su adopción generalizada. En el ámbito militar, la IA con agentes puede actuar como facilitadora analítica, multiplicadora de fuerza y disruptora, ofreciendo beneficios potenciales tanto para acciones ofensivas como defensivas. El desarrollo de la IA con agentes está dando lugar al concepto de guerra con agentes, en la que estos podrían proporcionar ventajas en el campo de batalla desempeñando funciones cada vez más importantes en ámbitos militares como la recopilación y el análisis de inteligencia, la planificación, la logística y la toma de decisiones. El uso de la IA con agentes amplifica ciertos desafíos presentes en los sistemas de IA actuales e introduce diversos riesgos y vulnerabilidades novedosos, especialmente en entornos de alto riesgo como el ámbito militar. Antes de su despliegue a gran escala, es crucial evaluar la trayectoria de la tecnología y sus posibles implicaciones para el futuro de la guerra.

Este análisis prospectivo explora cómo se desarrolla la IA con agentes en medio de la competencia comercial y militar por su adopción y la creciente rivalidad geopolítica. La tecnología y su integración en sistemas comerciales y militares tienen importantes implicaciones para la seguridad internacional y la estabilidad estratégica, y plantean interrogantes sobre su proliferación y uso indebido. A pesar de la mejora de las capacidades autónomas, los prometedores casos de uso y los diversos beneficios previstos, los agentes cada vez más autónomos también generan importantes riesgos sociales, de seguridad, legales y éticos que podrían poner en peligro la implementación exitosa, efectiva y sostenible de la IA con agentes si no se abordan. Esto exige que quienes buscan aprovechar el potencial de los agentes de IA encuentren un equilibrio entre autonomía y seguridad. Asimismo, requiere atención regulatoria y mitigación de riesgos mientras la tecnología aún se encuentra en sus primeras etapas y antes de su despliegue a gran escala.

https://www.gcsp.ch/sites/default/files/2026-04/GP-2026_37_Rickli%20Knappe_The%20International%20Security%20and%20Military%20Implications%20of%20Agentic%20AI%3Bdigital.pdf

<https://thelivinglib.org/from-search-engines-to-ai-agents-interface-control-and-the-restructuring-of-communication-power/>



CIBERCONFIANZA

Los videos IA y deepfake

Los avances en inteligencia artificial (IA) han facilitado la creación de vídeos deepfake altamente realistas, que pueden mostrar a alguien haciendo o diciendo algo que en realidad no hizo ni dijo. Los deepfakes pueden representar una amenaza para los individuos y la sociedad: por ejemplo, pueden utilizarse para influir en las elecciones desacreditando a los oponentes políticos.

La investigación psicológica muestra que la capacidad de las personas para detectar vídeos deepfake varía considerablemente, lo que nos hace potencialmente vulnerables a la influencia de un vídeo que no hemos identificado como falso.

Sin embargo, aún se sabe poco sobre el impacto potencial de un vídeo deepfake que ha sido explícitamente identificado y marcado como falso. Examinar este tema es importante porque las iniciativas legislativas actuales para regular la IA enfatizan la transparencia. Presentamos tres experimentos preregistrados ($N = 175, 275, 223$), en los que se mostró a los participantes un vídeo deepfake de alguien que parecía confesar haber cometido un delito o una transgresión moral, precedido en algunas condiciones por una advertencia que indicaba que el vídeo era un deepfake. Posteriormente, se les hicieron preguntas a los participantes sobre la culpabilidad de la persona, para examinar la influencia del contenido del video. Descubrimos que la mayoría de los participantes se basaron en el contenido de un video deepfake, incluso cuando se les había advertido explícitamente de antemano que era falso, aunque no se pueden descartar explicaciones alternativas para la influencia del video, relacionadas con el encuadre de la tarea. Este resultado se observó incluso en participantes que indicaron haber creído la advertencia y saber que el video era falso. Nuestros hallazgos sugieren que la transparencia es insuficiente para anular por completo la influencia de los videos deepfake, lo que tiene implicaciones para los legisladores, los responsables políticos y los reguladores del contenido en línea.

<https://www.nature.com/articles/s44271-025-00381-9>

<https://detectvideo.ai/>

[https://interestingengineering.com/innovation/china-builds-worlds-smallest-atomic-clock-for-drones?utm_campaign=13508169-](https://interestingengineering.com/innovation/china-builds-worlds-smallest-atomic-clock-for-drones?utm_campaign=13508169-The%20Blueprint%20Daily%20Subscription&utm_medium=email&hsenc=p2ANqtz--p9slGMYs2L9mhfo_7blwOAZhlhHJ5XFTOc1KDKbV--nz1E0gPHWKIOJQ6QFhuNLqGHhznmnDQ8kRgxXLQO7FrevhQnA&hsmi=409761742&utm_content=409761742&utm_source=hs_email)

[The%20Blueprint%20Daily%20Subscription&utm_medium=email&hsenc=p2ANqtz--](https://interestingengineering.com/innovation/china-builds-worlds-smallest-atomic-clock-for-drones?utm_campaign=13508169-The%20Blueprint%20Daily%20Subscription&utm_medium=email&hsenc=p2ANqtz--p9slGMYs2L9mhfo_7blwOAZhlhHJ5XFTOc1KDKbV--nz1E0gPHWKIOJQ6QFhuNLqGHhznmnDQ8kRgxXLQO7FrevhQnA&hsmi=409761742&utm_content=409761742&utm_source=hs_email)

[p9slGMYs2L9mhfo_7blwOAZhlhHJ5XFTOc1KDKbV--](https://interestingengineering.com/innovation/china-builds-worlds-smallest-atomic-clock-for-drones?utm_campaign=13508169-The%20Blueprint%20Daily%20Subscription&utm_medium=email&hsenc=p2ANqtz--p9slGMYs2L9mhfo_7blwOAZhlhHJ5XFTOc1KDKbV--nz1E0gPHWKIOJQ6QFhuNLqGHhznmnDQ8kRgxXLQO7FrevhQnA&hsmi=409761742&utm_content=409761742&utm_source=hs_email)

[nz1E0gPHWKIOJQ6QFhuNLqGHhznmnDQ8kRgxXLQO7FrevhQnA&hsmi=409761742&utm_content=409761742&utm_source=hs_email](https://interestingengineering.com/innovation/china-builds-worlds-smallest-atomic-clock-for-drones?utm_campaign=13508169-The%20Blueprint%20Daily%20Subscription&utm_medium=email&hsenc=p2ANqtz--p9slGMYs2L9mhfo_7blwOAZhlhHJ5XFTOc1KDKbV--nz1E0gPHWKIOJQ6QFhuNLqGHhznmnDQ8kRgxXLQO7FrevhQnA&hsmi=409761742&utm_content=409761742&utm_source=hs_email)

TECNOLOGÍA

Mapa de la industria militar de IA

La participación de la industria es una aspiración clave de las iniciativas de control de armamentos en lo que respecta a la aplicación responsable de la inteligencia artificial (IA) en el ámbito militar. Sin embargo, se presta poca atención a quién debería representar a la "industria" en estos procesos: qué empresas o segmentos de la cadena de suministro de IA del sector privado son relevantes para el contexto político.



Este documento informativo tiene como objetivo proporcionar una visión general de la industria de la IA militar para ayudar a los responsables políticos, así como a la sociedad civil y a los investigadores académicos, a comprender la amplia variedad de productos, actores y relaciones involucradas.

<https://www.brennancenter.org/our-work/research-reports/business-military-ai>

CIBERFORENSIA

Informes de Vulnerabilidades

En esta área hemos incorporado los informes semanales que proporciona la CISA (Cybersecurity & Infrastructure Security Agency) de los EEUU, estos boletines proporcionan un resumen de las nuevas vulnerabilidades que han sido registradas por la Base de Datos de Vulnerabilidad (NVD) del Instituto Nacional de Estándares y Tecnología (NIST).

2026

1. Vulnerabilidades semana del 20 de abril: <https://www.cisa.gov/news-events/bulletins/sb26-117>
 2. Vulnerabilidades semana del 27 de abril: <https://www.cisa.gov/news-events/bulletins/sb26-125>
 3. Vulnerabilidades semana del 04 de mayo: <https://www.cisa.gov/news-events/bulletins/sb26-131>
 4. Vulnerabilidades semana del 11 de mayo: <https://www.cisa.gov/news-events/bulletins/sb26-138>
-

EVENTO 55 Jornadas Argentinas de Informática (JAIIO)

- Ciudad de La Plata del 10 al 13 de agosto de 2026
- Primer Llamado a presentación de trabajos <https://55jaiio.sadio.org.ar/>
- Organizan: SADIO - Sociedad Argentina de Informática Universidad Tecnológica Nacional - Facultad Regional La Plata

Lecturas, Videos y Podcasts

1. Podcast Guerra Cognitiva: <https://global-strategy.org/guerra-cognitiva-i/>
 2. Operaciones en el Ambiente de la Información Libro en formato digital disponible en:
https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/CEFADIG_b2ce737fe7427cb279d7cb6ef4bd53c8
 3. La ciberseguridad es ahora una prioridad en las salas de juntas:
<https://www.youtube.com/watch?v=Jgu4VY7zyAg>
 4. La empresa agente: cómo los agentes de IA están transformando los negocios con Adam Evans de Sale..
<https://www.youtube.com/watch?v=bsxrTa9YL3Y>
-



Facultad
Militar
Conjunta



CYBER.AR
I CONGRESO DE CIBERDEFENSA
ARGENTINA 2026

16, 17 y 18 DE SEPTIEMBRE

TERCERA CIRCULAR

8 JUNIO Fecha límite de envío de resúmenes

24 JULIO Fecha límite de envío de resúmenes extendidos y trabajos completos

PRESENTACION
PAGINA OFICIAL Y CALL FOR PAPERS

Nos complace anunciar que ya se encuentra disponible la página web y la recepción de trabajos para el I Congreso de Ciberdefensa - Argentina 2026. En la página podrán encontrar el acceso al Microsoft Conference Management Toolkit para el envío de trabajos.

Los invitamos a presentar sus contribuciones originales dentro de las áreas temáticas de esta edición.

Toda la información referente a requisitos formales, plantillas de envío y criterios de evaluación se encuentra disponible para su consulta directa en nuestro sitio oficial.

www.cyberar.fie.undef.edu.ar

Logos: UNDEF, Facultad de Ingeniería del Ejército, Facultad Militar Conjunta, Instituto de Ciberdefensa de la Fuerza Armada Argentina

Copyright © * | 2026 | *

* | Facultad Militar Conjunta | *

Todos los derechos reservados.

* | Observatorio Argentino del Ciberespacio | *

Sitio web: <http://undef.edu.ar/fmc/ciberespacio/boletines.php>

Nuestra dirección postal es:

* | Luis María Campos 480 - CABA - República Argentina | *

Nuestro correo electrónico:

* | observatorioargentinodelciberespacio@conjunta.undef.edu.ar | *